~~SECRET~~

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM: [redacted] Executive Director	EXTENSION	NO. 25X1
		DATE 14 November 1985

TO: (Officer designation, room number, and building)	DATE RECEIVED	DATE FORWARDED	OFFICER'S INITIALS	COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)
1. DCI				Here's the still somewhat rough piece I promised this afternoon on the leaks question. You asked one question. I tried to answer that one and answered another one that you didn't ask. I'm not sure that what I've started here will be helpful to you in a meeting with the Attorney General. I'm becoming persuaded that while we should do everything we can to get others to help us, what we need to do now is turn to what is within our managerial ability to accomplish. The paper attached takes this tack. If what I'm suggesting here could be a basis for action with the Executive Branch, how would we deal with the Congress? My sense is that we should strive to push the Congress to match our action, or at least move toward being the only organization in town that doesn't act responsibly. Then you might be able to set in motion the forces to solve the problem. [redacted] 25X1
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

FORM 1-79 **610** USE PREVIOUS EDITIONS

~~SECRET~~

GPO : 1983 O - 411-632

DRAFT SECRET

14 NOV 1985

NOTE FOR: DCI

DDCI

SUBJECT : "More on Leaks"

1. You asked that I give further thought to my earlier suggestion that we try, as part of an attack on leaks, to reduce significantly the volume of raw intelligence data and finished intelligence product circulating outside the Agency or the intelligence community.

2. Here are thoughts on how we might proceed:

- First, divide the problem up functionally and identify individual managers who will develop strategies to reduce the dissemination of: (1) DDI analytic products (Bob Gates), (2) raw human intelligence (Clair George), (3) raw SIGINT intelligence (Bill Odom), (4) raw imagery reports (Rae Huffstutler), and (possibly) (5) materials relating to the covert action decision-making process.

- Second, start by working on products under our direct management control in the DDI and the DDO, leaving NSA and NPIC for later. (NSA and NPIC need to be dealt with somewhat differently because they both respond directly to military as well as to civilian requirements.)

- Third, set a specific, ambitious, goal in each area, perhaps a 30 percent reduction in the number of copies of each and every individual report disseminated.

3. To be more specific:

- For the DDI, I would ask Bob Gates to take yet another look at the distribution of our publications, with the goal of reducing by 30 per cent the number of copies distributed to Defense, State, and elsewhere. Do this, recognizing that such an arrangement will probably result in someone somewhere not getting what he needs, that it will produce screams of anguish, that it will probably generate a certain amount of unauthorized Xeroxing, and that it will force us to devote much more effort to considering precisely who must see what, i.e., it will push

all of us to tighten up our attitudes about "need to know." Be prepared to hold to such a scheme for an extended period without caving under the pressures in order to allow those who can finally see how life can go on under the new rules to come to the fore. Recognize that State and Defense will mostly have to tell us who must have access to what, and that we'll need their cooperation.

- For the DDO, I would ask Clair George to assemble a group who would work with other agencies to reduce (again by 30 percent) the number of copies those other organizations distribute of our electronically disseminated products. This, of course, won't be easy, having as its objective a revision of the whole network of dissemination practices in other agencies which have evolved over the years.

- Both the DI and DO proposed programs imply that we tell other agencies to design internal document control programs which meet specific standards set by us or risk losing continued access to our products. Therefore, our Office of Security should be deeply involved in developing tight certification rules. We should consider expanded use of sensitive document reading rooms as a step toward document control, as an overt sign to everyone that the rules have changed, and possibly as part of a decision to establish a category of information which cannot be seen without a signed statement that the author agrees to be polygraphed if a subsequent leak should require it.

- In addition to the certification program, ask the Office of Security to develop an effective audit program to assure other agencies' compliance with our new rules. As noted above, a major side effect of an effort to clamp down on the "officially sanctioned" dissemination of our products could well be an increase in the amount of Xeroxing. An aggressive security audit program of some kind would help to control this tendency.

- Finally, issue regular "progress" reports to Bill Odom, Rae Huffstutler and others, both to let NSA and NPIC know that in due course we will ask them to undertake the same program, and at the same time to build pressure elsewhere for similar efforts.

4. Of course, our basic mission is to make intelligence available to those who need it. Also, we know that most (perhaps nearly all) of our serious leaks have come from papers or briefings given, because of their sensitivity, only to sharply limited numbers of people. You may recall that we examined many of these issues a year ago in a report to you by an Agency Task Force on Dissemination (copy attached). At that time, after a detailed look at our dissemination of all raw and finished intelligence, we concluded that there was little evidence that an arbitrary reduction in the volume of such disseminations would help with the leak problem. We noted, reconfirming most of our previous experience, that our serious leaks can nearly always be traced to that group of people who receive our most sensitive information in the form of: [redacted] (2) DI NID's, (3) DI "Ad Hoc's," and (4) briefings from both the DO and the DI. 25X1

5. In the face of this, would the program sketched out above still make sense? I think so. A purposeful effort to greatly reduce the amount of raw and finished intelligence circulating would:

- help us regain the initiative with respect to leaks;
- strengthen our ability to ask others to take difficult steps;
- ultimately improve our ability to deliver our intelligence to those who most need it;
- probably help some impact on the numbers of leaks--if only by reducing the numbers of people journalists can canvass to verify or amplify information they may already have obtained;
- help us get the attention of hundreds of individuals in the Executive Branch and on the Hill, allowing us to make more important changes at the same time.

6. In reviewing this issue once again, I asked myself the following questions: are we doing everything within our power and authority to ensure that those who do receive our most sensitive materials are properly conditioned to the importance of secure handling? When violations do occur, do we do everything we can to ensure that they don't reoccur?

7. I think it is fair to say that much has been done. But there is room for considerably more progress--particularly in light of the additional (polygraph) authority which it appears you have under NSDD 196--if you accept the following three assumptions:

- We need to get serious about applying the principle of "need-to-know" to a larger proportion of our total output than is the case today. Doing this will be costly, and in fact runs counter to much current practice.

- We need to revitalize the notion that access to sensitive material is a privilege, not a right.

- Third, our real power to get others to pay attention to our security requirements rests on our ability to deny access to our intelligence. But we can't even deny access if we don't exercise greater physical control over the intelligence as it is disseminated.

8. Here are a few further suggestions for how we might deal with the problems we face from an alarming number of leaks of highly sensitive information:

- First, create a class of information which requires a signature in order that it be seen, which establishes that the recipient agrees that he has been given access to privileged information, and that if a subsequent leak should justify it, he agrees to a non-lifestyle polygraph. This might be SCI information, or some significant part of that now considered SCI.

- Second, further extend the well-established "personal accountability" features successfully employed by the DI [redacted], and by the DO [redacted] In particular, add a new dimension of personal accountability to the handling of all SCI materials, which currently must be examined in special SCI facilities. (Attachment IV of last year's Task Force on Dissemination explains how the current SCI control system works.) More can be done (it will cost) to apply much more strictly the need-to-know principles for access to special compartmented information.

25X1
25X1

- Third, consider greatly reducing our use of briefings as a means of conveying information.

9. In last year's Task Force report, we particularly flagged our use of briefings as a problem area, and recommended to you that we take all feasible steps to "...hold briefings on sensitive subjects to an absolute minimum. Where such briefings are necessary, details of briefing contents and the audience for the briefing should be closely controlled and fully documented."

10. We further noted that we had lots of questions about why there seemed to be such a large percentage of leaks traceable to briefings, including this one: "Are briefings, by their give and take nature and by the fact that security caveats are spoken rather than constantly before the eyes of a reader, an inherently less secure form of disseminating information? Do briefings generate leaks?"

11. Of course, briefings are a very useful tool in our kit bag. But for reasons that we may not fully understand, they do seem to generate a significant portion of our leaks. Because we might learn something important, I would consider establishing in the Agency a central point to review virtually every substantive briefing to be given outside the Agency from a sources and methods point of view. This could only work if it were jointly staffed by the DO and the DI, and perhaps in some cases the S&T, and if there were hardly any exceptions to its rules. It would require at least the full-time attention of several senior people. But a review process could bring greater consistency to aspects of the external presentation of intelligence and certainly to the way we handle sources and methods issues. A major function of such a group would be to recommend or decide that a given subject should not be briefed at all, but that a written presentation should be prepared instead. This could often give us important breathing room on today's issue, and could help us dampen emotions as well.

12. With fewer briefings, more careful control of a larger percentage of our sensitive paper, a better paper trail of information on individuals who have received sensitive information, and agreement by those who have received such information that they will submit to a polygraph if required, the crucial remaining task is to ensure that something is done when a leak occurs. I would suggest that we have enormous leverage here, if we are willing to employ it. Some of the possibilities include:

-- A personal letter from you or someone here to the suspected leaker, telling him that we have certain facts in our possession and that he will no longer have access to any classified information made available by us unless he can persuade us our judgment is wrong.

-- A letter from you to the President to note that you have derogative information about an individual and you have decided that your sources and methods authority requires you to deny him future access to classified information.

-- And, of course, a request to the Attorney General to prosecute or to take other appropriate legal action.

13. In short, I think it's time that we consider sanctions derived from your legal authority to protect sources and methods, grounded in our belief that access to sensitive classified information is not a right, but a privilege, and based upon the fact that this is something which is within our management authority to do. Some will argue that a decision to cut off intelligence potentially means we are accepting the notion that a possible leaker is guilty until proven innocent. But it seems to me this kind of thought assumes that a customer has rights, or at least that his right of access outweighs our responsibility to protect sensitive intelligence. Shouldn't we question this assumption?

25X1